Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 6636665, 16 pages
https://doi.org/10.1155/2021/6636665

Review Article

A Survey of User Authentication Based on Channel State Information

Zhengjie Wang, Wenwen Dou, Mingjing Ma, Xiaoxue Feng, Zehua Huang, Chengming Zhang, Yinjing Guo, and Da Chen

College of Electronic and Information Engineering, Shandong University of Science and Technology, Qingdao 266590, China

Correspondence should be addressed to Zhengjie Wang; cieewangzj@163.com and Yinjing Guo; gyjlwh004@126.com

Received 14 December 2020; Revised 11 March 2021; Accepted 2 June 2021; Published 16 July 2021

Academic Editor: K. Shankar

Recently, human behavior sensing based on WiFi channel state information has drawn more attention in the ubiquitous computing field because it can provide accurate information about the target under a device-free scheme. This paper concentrates on user authentication applications using channel state information. We investigate state-of-the-art studies and survey their characteristics. First, we introduce the concept of channel state information and outline the fundamental principle of user authentication. These systems measure the dynamic channel state information profile and implement user authentication by exploring the channel state information variation caused by users because each user generates unique channel state information fluctuations. Second, we elaborate on signal processing approaches, including signal selection and preprocessing, feature extraction, and classification methods. Third, we thoroughly investigate the latest user authentication applications. Specifically, we analyze these applications from typical human action, including gait, activity, gesture, and stillness. Finally, we provide a comprehensive discussion of user authentication and conclude the paper by presenting some open issues, research directions, and possible solutions.

1. Introduction

Recently, human behavior sensing has drawn considerable concern and achieved important research progress in the field of ubiquitous computing. With these behavior recognition applications, we can acquire users' behavior states and infer their daily movement regularity, which provides us with an effective means to understand users' actions. In addition, device-based approaches [1, 2] usually require users to carry sensors, which creates some deployment difficulty and restrains their use field. Therefore, this paper focuses on the device-free approach. Traditionally, human behavior recognition applications can employ many types of signals, including vision [3–5], sound [6–9], light [10, 11], and RF (radio frequency) signals. Specifically, popular RF signals include RFID (radio frequency identification) [12–14], radar [15], and WiFi signals [16–19]. Each signal has its advantages and disadvantages; therefore, we should select an appropriate signal based on application requirements. This paper focuses on human behavior with the WiFi signal. Currently, WiFi signals can be measured using COTS (commercial off-the-shelf) devices, such as an Intel 5300 NIC (network interface card) [20], an Atheros 9580 [21], a Raspberry Pi [22], and an ESP32 [23]. Many studies have confirmed the feasibility of utilizing the WiFi signal to realize behavior sensing and have achieved many attractive research results. Some surveys have summarized state-of-the-art studies and presented insight into further research trends [24–26].

WiFi device usually provides two kinds of signals: CSI (channel state information) and RSS (received signal strength). RSS stands for the strength of the received signal and was utilized in [27–32]. CSI refers to channel state information that describes the channel properties of a communication link. Compared to RSS, CSI can provide more fine-grained information. In recent years, CSI-based human behavior technology has become popular. Therefore, we are interested in CSI-based applications in this paper. The representative applications include action recognition [33–35], indoor localization [36, 37], fall detection [38, 39], keystroke detection [40, 41], breath detection [42, 43], smoking detection [44], human flow estimation [45, 46], and human gesture recognition [47–49].

Among the human behavior sensing applications, we are interested in a specific application, user authentication. With growing concern about security problems, there is an urgent need for a nonintrusive and simple user authentication approach [50]. Currently, many user authentication applications have achieved satisfactory research achievements. Similar to behavior recognition, these applications explore CSI variation to implement user authentication. Although both behavior recognition and user authentication leverage signal variation to implement recognition, the leading considerations are different in recognition procedures. The key to behavior recognition applications is to identify different actions and eliminate the effect of different users on CSI signal variation. In contrast, the core of user authentication is to determine the identity of different users and mitigate the effect of specific actions on recognition. Currently, many different applications employ different actions. Specifically, these actions include gait [51, 52], activity [53, 54], gesture [55], and stillness [56, 57]. In addition, these CSI-based user authentication systems include two types of applications. One determines the identity of a user in the training set. The other determines whether a user is a stranger or an intruder. From these applications, we find that the former needs to assign a label to the unknown using known labels, while the latter only requires a binary answer, is or not. As a result, we can classify typical user authentication systems into these two categories, i.e., applications identifying a user's identity [58], while other applications can recognize a stranger [59].

Based on the above statement, CSI-based user authentication techniques have been studied and have achieved satisfactory performance. However, there is no survey to review these applications and present insights into the research. This paper emphasizes user authentication and analyzes its key components. It surveys the typical CSI model and summarizes the various applications. In addition, it categorizes these applications and compares them from different activity types. We hope that this article can make a comprehensive summary of the existing CSI-based user authentication applications and provide some helpful information about the current state and future development direction.

The main contributions of this paper can be summarized as follows. This paper investigates and presents a comprehensive survey of the latest user authentication applications based on CSI variation. First, we present the principle of CSI-based user authentication and analyze the signal processing methods used in user authentication applications. Second, we investigate the latest user authentication applications and conduct a comprehensive survey of their characteristics. Third, we present a detailed discussion, current issues, and future research trends.

The rest of the paper is organized as Figure 1. In Section 3, we discuss the principle of channel state information and user authentication based on CSI. Section 4 presents the methods of signal selection and preprocessing, feature extraction, and classification methods. Section 5 investigates the latest applications of the user authentication technique based on WiFi CSI. In Section 6, we discuss some factors that influence authentication accuracy. Section 7 presents the challenges, future research trends, and open issues. In Section 7, we reach a conclusion.

2. The Principle of Channel State Information and User Authentication Based on CSI

User authentication is an important research topic in the human behavior recognition field and has achieved significant research progress. Specifically, this method provides a simple and nonintrusive authentication pattern without disturbing the users' normal movement, making long-term monitoring available. In this section, we introduce the concept of CSI, provide the fundamental principle of user authentication, and present the system architecture of typical applications.

2.1. Channel State Information. CSI describes the channel state of wireless communication links and is designed to evaluate communication links' quality. In addition, it comes from the physical layer of NIC and provides the phase and amplitude information of each subcarrier. Because every subcarrier is independent of each other, the multipath effect of different subcarriers has a distinct reaction on the phase and amplitude. Therefore, movements with different ranges can be detected by different subcarriers, which means that CSI can distinguish different granularities of action. As a result, CSI can realize higher action recognition since it can recognize more fine-grained actions, such as breathing and heartbeat. In the frequency domain, the wireless channel state can be described as:

$$Y = H \times X + N, \tag{1}$$

Y, X, H, and N represent the received signal vector, transmitted signal vector, channel matrix, and Gaussian white noise, respectively. The channel matrix describes the attenuation factor of the signal in each transmission path, and the value of each element in the channel matrix contains information such as signal scattering, environmental attenuation, and distance attenuation. The channel matrix is described as:

$$H_i = |H_i| e^{j \sin(\angle H_i)}, \tag{2}$$

where the first term is the value of CSI for the i^{th} subcarrier, and it contains the amplitude and phase information. On the right side of this equation, $|H_i|$ and $\angle H_i$ represent the amplitude and phase information of the i^{th} subcarrier, respectively.

In addition, the IEEE 802.11 [60] standard is realized by most commercial WiFi devices, and it utilizes multiple antennas to implement MIMO (multiple input multiple output) communication. Standard WiFi devices work at 2.4 GHz and 5 GHz bands, and they use an OFDM (orthogonal frequency division multiplexing) signal modulation scheme in the PHY (physical) layer. WiFi CSI continuously detects the frequency response of OFDM subcarriers and captures various environmental changes, such as frequency selective fading, shadowing, multipath, destructive, and constructive interference. Based on these signal changes, we can identify human identity by exploiting the pattern of each user movement.

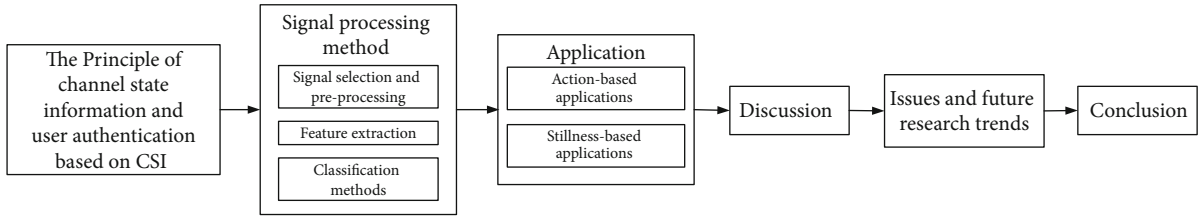

Figure 1: The flowchart of this paper.

2.2. The Principle of User Authentication Using CSI. The fundamental principle of user authentication is that different users can generate unique CSI variation when a user is located in the coverage of the CSI signal. Therefore, we can recognize a user's identity by exploiting the dynamic CSI profile. To our knowledge, there are two main types of user authentication based on whether the user moves. One utilizes the dynamic CSI caused by user movements. According to the magnitude of the actions, these movements can be divided into gait, activity, and gesture. These approaches are widely employed because human movement can generate evident CSI fluctuations that can be measured and processed by exploring many available algorithms. We refer to the method as an action-based approach. Even though conducting the same activity, different people have distinct impacts on channel changes due to the behavioral characteristics of every one. In addition, various factors, such as a user's height, weight, action speed, action rhythm, action range, and waving cycle, affect CSI signal propagation, which generates a unique CSI profile. The other utilizes the static propagation feature of CSI when the user remains still. This approach can identify people according to the user's physiological characteristics, such as the water rate, fat rate, and muscle rate of the user. It builds a unique CSI signal profile based on user biometric features. This approach can also identify people by the combination of location and user. It creates a unique CSI profile based on the correlation between these two factors. In addition, some applications apply respiration or lip motion for authentication. We refer to these methods as stillness-based approaches. Compared to action-based user authentication, stillness-based user authentication has challenging problems in extracting unique features.

2.3. The Framework of CSI-Based User Authentication. Currently, CSI-based user authentication has achieved great success by exploring dynamic CSI variation. Although we can categorize these applications into different groups from many aspects, such as action types and recognition methods, the framework of these applications is simple and clear. We divide the signal procedures into the following parts: signal collection, signal selection and preprocessing, feature extraction, and classification, as shown in Figure 2. Specifically, the signal collection realizes CSI data measurement. We usually deploy a standard AP (access point) to send data packets and apply a laptop running a modified NIC driver to collect CSI data. Usually, CSI is used to assess the communication link and cannot be measured with the common application. Therefore, to acquire CSI data, we have to modify the NIC driver to transfer the CSI data to application layers. The data collected usually contain much noise from ambient factors or hardware devices; therefore, the data usually cannot be used immediately. We need a vital step called signal preprocessing to suppress the noise, eliminate outliers, and smooth the abrupt data. We usually employ filters, PCA (principal component analysis), DWT (discrete wavelet transform), and interpolation to obtain more precise data. After that, we need to segment the CSI stream and obtain a series of data sequences describing an action cycle. Therefore, we can obtain the full description of each action from the sequences. To obtain the features that can represent the action, we need to conduct feature extraction. We may select statistical features to illustrate the actions with some simple parameters. We can also utilize the time-frequency diagram as a feature description because it holds much information. Finally, we identify the user's identity based on the classification algorithms. We usually utilize machine learning or deep learning algorithms, such as KNN (K-nearest neighbor) [61], SVM (support vector machine) [59, 62], DTW (dynamic time warping) [51], CNN (convolutional neural network) [53], DNN (deep neural network) [63], GRU (gated recurrent unit) [52], and LSTM (long short-term memory) [64], to validate the user's identity.

In this section, we present the concept of CSI, the principle of user authentication, and the framework of the user authentication system using CSI. Based on the introduction, we can understand the critical characteristics of the system and are familiar with the components and their function. We analyze in detail the key content of the system and elaborate on the specific function of each component in the following parts.

3. Signal Processing Method

In this section, we illustrate the signal processing procedures for some user authentication applications. Raw CSI signals need to be processed to obtain useful information. Many crucial steps need to be carried out, including signal selection and preprocessing, feature extraction, and classification. Next, we introduce a specific working process.

3.1. Signal Selection and Preprocessing

3.1.1. Signal Selection. Signal selection plays a vital role in user authentication since it has a significant influence on accuracy. As described in Section 3.1, CSI data can be represented as a channel matrix, including amplitude and phase information. Existing user authentication systems usually

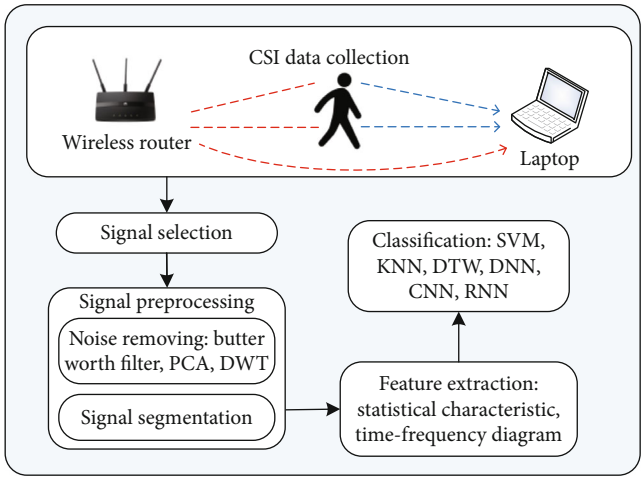

Figure 2: The user authentication framework.

select amplitude or phase as the base signal to conduct the subsequent signal processing.

Most systems applied amplitude information to realize user authentication because various actions in the WiFi area will cause amplitude changes in the receiver [65]. In addition, some other systems utilize phase information. For example, CP-ID [66] applied phase information to capture finer changes compared with amplitude. However, the phase of the signal needs to be calibrated to remove various noise and distortion. Furthermore, the combination of amplitude and phase information was also used to recognize signal variation, such as HumanFi [64]. This approach can take advantage of amplitude and phase to achieve more accurate identification.

3.1.2. Noise Removing. Preprocessing is a necessary step after collecting CSI signals. In experiments, we find that the raw CSI provided by commodity WiFi NICs is noisy because of the complicated surroundings and reflections of many objects. Therefore, we must remove noise in signals to obtain a clean signal for the next processing step. Typical signal preprocessing methods, such as PCA, Butterworth filter, and DWT, are often used to remove noise.

The Butterworth filter is a common method for removing high-frequency noise. For example, in WiFi-ID [65], the authors adopted the Butterworth filter to remove high-frequency noise. Due to its smoother passband responses compared to other filters, it achieved excellent filter results.

In many studies, they also utilize PCA to implement noise removal. The main idea of PCA is to map the n -dimensional features to the k-dimension, which is a new feature named a principal component. Generally, this preprocessing approach has two advantages. The first can reduce the dimensionality of the CSI information obtained and decrease the computational complexity. The other can remove noise in signals efficiently by taking advantage of correlated variations in the CSI time series of different subcarriers. Furthermore, it can remove uncorrelated noisy components, which cannot be removed through traditional low-pass filtering [40].

Wavelet transforms can not only describe the frequency-domain features of local time-domain processes but also obtain the time-domain features of local frequency processes compared to the traditional cosine transform. It can transform the image into a series of wavelet coefficients to compress and store images efficiently. In addition, the rough edges of the wavelet can represent the image better because it eliminates the block effect in DCT (discrete cosine transformation) compression. In WiID [67], after denoising by a low-pass filter, PCA and DWT were used to obtain the waveform characteristics of the data.

3.1.3. Signal Segmentation. Signal segmentation is aimed at splitting the data streams into a series of sequences that describe a whole action conducted by the user. Compared to device-based methods, it is more difficult to detect the start point and endpoint of a stream because these signal changes of action periodicity are weak for device-free approaches.

In WiFi-ID [65], the authors proposed that determining effective regions with suitable lengths is necessary. They identified the approximate midpoint of the effective region first. Then, they determined the starting point of the valid region. Specifically, the authors segmented the stream into a short frame and calculated the short-time energy of each frame. They smoothed the vector that represents the short-time energy of all frames, and this vector was used as the threshold of the central region. In addition, they selected the original signal corresponding to a contiguous block of frames in which each frame was above the threshold as the central region. The midpoint, m, was the instantaneous signal that has the maximum deviation from the average in the central region. The duration of the effective region was T. Therefore, the starting point is located in $(m - T)/2$. Finally, they obtained the effective region by the midpoint and starting point.

In Wii [59], the authors proposed that the combination of CWT (continuous wavelet transform) and wavelet variance can effectively discover the periodicity of the CSI waveform. FreeSense [51] designed a segmentation algorithm based on MAD (mean absolute deviation). This algorithm adopts a sliding window approach to search segmentation points. Similarly, Hong et al. [62] also applied the sliding window approach to detect the starting and ending points. In the BioID [68], the authors determined the starting and ending points of the lip movements by setting thresholds. In addition, the thresholds were experimentally determined.

In general, this section includes three parts: signal selection, noise removal, and signal segmentation. First, both the amplitude and phase will change during signal propagation. The amplitude, phase, or combination of the two can be used as basic signals in many user authentication systems. Second, noise removal is aimed at eliminating irrelevant information and saving useful information reflecting human behavior details. Third, most signal segmentation algorithms segment the effective area of the signal by determining the starting point, midpoint, or ending point of the CSI data stream. After signal selection and preprocessing, CSI signal information can be extracted to obtain useful features.

3.2. Feature Extraction. After preprocessing, we can extract the main features from the filtered signals. Feature extraction is a signal processing procedure in which we select some major features from data to more accurately depict the data because the original data usually contain more redundant information. Generally, we extract useful features depicting CSI variation caused by distinct users, such as statistical features and time-frequency diagrams.

3.2.1. Statistical Feature. Statistical features are common feature descriptions for measurement data and can be calculated by using a statistical formula. It depicts the general characteristics of the data and is widely used in pattern recognition applications. Specifically, the statistical features of the CSI signal can be divided into time-domain features and frequency-domain features. The time-domain features are extracted directly from the original waveform, while the frequency-domain features are extracted after the FFT (fast Fourier transform) of the original waveform. Wii [59] calculated the statistical features of the time domain and entropy of the frequency domain reflecting per-step and walking features.

3.2.2. Time-Frequency Diagram. The time-frequency diagram can depict the data features from the time and frequency domains. Specifically, by using STFT (short-time Fourier transform), time signals are transformed into a time-frequency diagram that can obtain more abundant information. We can obtain information on the moving speed of different body parts from the time-frequency diagram by analyzing the frequency changes over time. The spectrogram in Figure 3, from WifiU [69], exhibits a scenario in which a user walks in a straight line. We find that the signal energy reflected by the torso is stronger than that of other body parts since the torso has a larger reflection area. Consequently, the time-frequency diagram can provide useful information about the human walking pattern.

By feature extraction, we can obtain useful information that can reflect a user's unique characteristics. This will improve the efficiency of user authentication. In most existing systems, the authors extract statistical features or time-frequency diagrams from CSI signals that reflect behavior features in the time and frequency domains.

3.3. Classification Methods. After feature extraction, a user's identity can be authenticated based on the extracted feature of CSI. Authentication methods are aimed at identifying a user's identity. Therefore, user authentication can be considered a classification problem and apply general classification approaches used for behavior recognition. In the classification process, we often use some typical methods, such as SVM, KNN, DTW, CNN, DNN, and RNN (recurrent neural network).

3.3.1. Machine Learning Technique. SVM is a kind of generalized linear classifier to classify binary data based on a supervised learning method. SVM splits the data into two groups using hyperplane. In user authentication based on CSI, SVM is also an effective classification approach and is widely utilized. For example, CareFi [70] applied SVM to determine whether a user is a stranger or an authenticated user.

K-nearest neighbor means that its closest K neighbors can represent the sample. The main processes of this algorithm compare the characteristics of the test data and training data based on knowing training data and labels. KNN is more suitable than SVM in the multiclassification problem. Therefore, researchers often choose KNN to process the multiclassification problem in user authentication. For example, FreeSense [51] achieved satisfactory identification accuracy in indoor environments.

DTW is a simple and efficient algorithm to compare the similarity of two-time series by extending and shortening the displacement of the time series. DTW is also employed in user authentication applications. For example, FreeSense used DTW to find the minimum distance alignment between two waveforms of different lengths and calculate the similarity between them [51].

3.3.2. Deep Learning Technique. DNN, also called a multilayer perceptron, is a deep neural network that improves classification efficiency successfully compared to the approach of traditional machine learning. As shown in Figure 4, it contains three parts: an input layer, some hidden layers, and an output layer. Any neuron in the former layer is connected to a neuron in the latter layer. In reference [63], they applied a DNN based on AutoEncoder to classify users, which improved the computational efficiency and robustness.

CNN is a kind of feed-forward neural network with a deep structure and convolution computation. As shown in Figure 5, the structure of CNN contains the input layer, convolutional layer, pooling layer, fully connected layer, and output layer. Specifically, the convolutional layer can extract features from large amounts of data. The number of convolution kernels, the stride, and the padding have an important effect on the output of the convolution layer. The pooling layer mainly plays a role in data dimensionality reduction to facilitate data calculation and storage. The output of the fully connected layer can be used as the input of the classifier. WiAU [53] applied CNN to implement user authentication. It combined CNN and ResNet algorithms to achieve fast and efficient user authentication.

Compared to CNN and DNN, RNN gives the network a kind of memory function of the previous content. Specifically, the current output of a sequence is also related to the previous output. Although RNN can handle time-series well, there are still some problems (vanishing gradient and exploding gradient). Fortunately, LSTM and GRU, variants of RNN, can solve these problems.

LSTM realizes the retention of important content and the removal of unimportant content by using the structure of the gate. There are three gates in an LSTM cell, i.e., input gate, forget gate, and output gate. The specific structure of LSTM is shown in Figure 6. LSTM is used in user authentication and has recently achieved great performance, such as HumanFi [64]. GRU is similar to LSTM, which also uses a gate structure to control memory and input. As shown in Figure 7, it contains a reset gate and an update gate. In user authentication, GRU is also applied and has high identification accuracy, such as Deep-WiID [52].

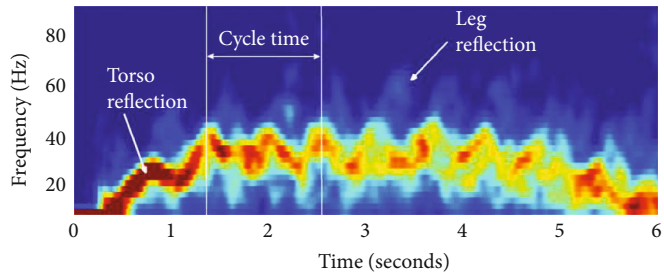

Figure 3: CSI spectrogram with human walking [69].

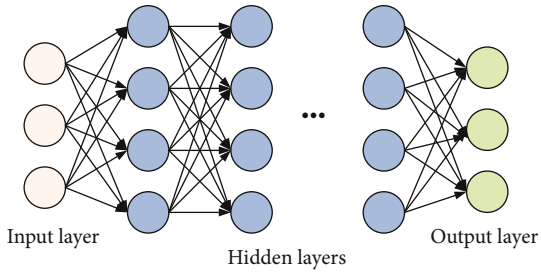

Figure 4: The illustration of DNN.

Classification methods play an important role in user authentication applications because the authentication process can be considered a classification problem. Based on the investigation of typical applications, we find that machine learning techniques are used widely in these existing studies since they are general classifiers and can work well for most classification questions. Furthermore, deep learning techniques are also leveraged in many authentication applications because they can automatically extract latent features and process high-dimensional data, which is very effective for complex CSI signal variation. By comparing the recognition performance of these two methods, we found that the method based on deep learning can achieve higher accuracy.

4. Application

With the advance in computing technology and the popularity of WiFi devices, CSI signals from WiFi devices are drawing more attention, and related user authentication applications are increasingly emerging. Human action within the coverage of WiFi can attenuate signal power and change the signal propagation path, which leads to a multiple-path effect. Furthermore, the impact on CSI is different when different people perform the same action. Therefore, the difference in the CSI signal caused by different users can be identified to recognize the user's identity.

Some crucial aspects should be considered when we analyze user authentication in detail. First, when analyzing typical applications, we must consider the test scenario because identification performance is related to the test environment. Most tests are conducted in indoor environments. There are also special scenarios, such as in-car and ramp. In addition, to evaluate the robustness of systems, authors usually ask users to perform the actions in one to four test environments. Second, from the function of user authentication, the existing user authentication system can determine the identity of a certain user in the group or identify strangers who do not belong to the group. Third, we also consider the number of participants because it exerts a significant effect on recognition accuracy. Fourth, since signal preprocessing methods are related to the CSI signal, we put them into one column in the following tables. Similarly, we also put the purpose of systems and the classification methods into one column in the tables. Since most systems employ the Intel 5300 NIC to measure the CSI signal, we do not display the test devices in the tables when analyzing these systems. Next, we enumerate these user authentication systems based on two approaches, i.e., action-based and stillness-based.

4.1. Action-Based Applications. Action-based user authentication has been widely applied because coarse-grained actions can cause more obvious changes in CSI and implement higher recognition accuracy. In this section, we introduce action-based user authentication systems from the aspects of gait-based, activity-based, and gesture-based systems.

4.1.1. Gait-Based. User authentication based on gait has made great progress in recent years. These applications identify a user's identity according to different walking gestures since everyone has a unique gait. Currently, most of the existing studies leverage gait to determine human identity. As shown in Table 1, many factors are investigated, including experimental environments, volunteers, preprocessing and classification methods, and identification performance. Next, we analyze some typical gait-based user authentication applications.

FreeSense [51] is a user authentication system based on gait features. In the process of identification, the authors adopted a Butterworth IIR filter to remove noise. Then, they used PCA to reduce the dimensionality of the data. Furthermore, they designed a signal segmentation algorithm and applied DWT to conduct feature extraction. Finally, they applied KNN based on DTW to classify users. The experimental environment is shown in Figure 8. Specifically, the transmitter and the receiver equipped with an Intel 5300 NIC were placed on the doorway 250 cm apart, and volunteers were required to walk along the straight line. Through extensive experiments, FreeSense achieved an accuracy of identifying one person from 94.5% to 88.9%, with people ranging from 2 to 6. Different from FreeSense, Deep-WiID [52] is a gait-based user authentication system using deep

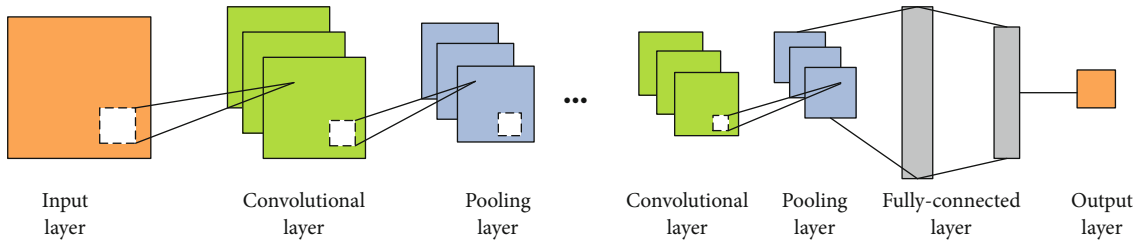

Figure 5: The illustration of CNN.

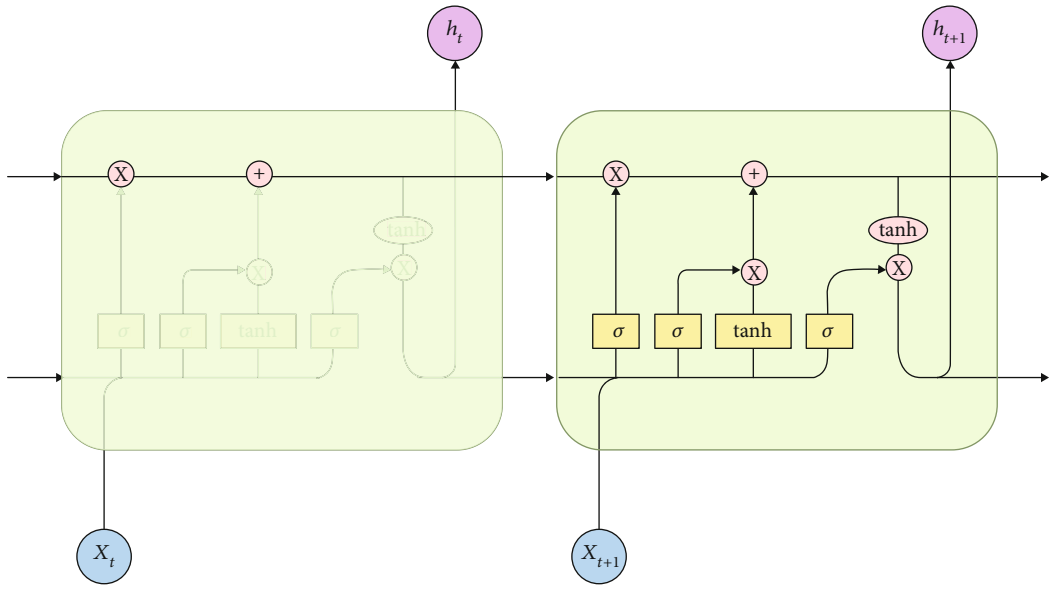

Figure 6: The illustration of LSTM.

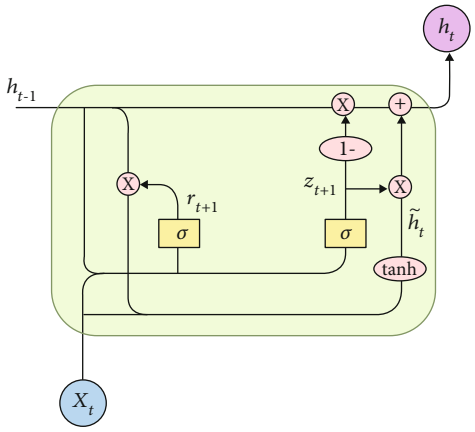

Figure 7: The illustration of GRU.

learning techniques. In addition, it is worth noting that Deep-WiID saves some preprocessing work. The CSI time series selected by the sliding window from raw CSI data is put in the network. This network is composed of a GRU layer, pooling layer, and classification layer. By training the deep neural network, Deep-WiID realized the accuracy of identifying one person from 99.7% to 97.7% with people from 2 to 6.

Some applications realize better performance in the number of identified people. For example, WifiU [69] can identify 50 participants using the LibSVM tool with the RBF (radial basis function) kernel. In addition, Neural Wave [74] and HumanFi [64] can identify 24 and 30 people, respectively.

In addition, some applications can identify strangers who do not belong to the training set, and it is a significant application in the field of user authentication. For example, Wii [59] not only identifies people in the training set but also realizes stranger identification. It realized recognition accuracy of 1 person with 98.7% to 90.9% from 2 to 8 people, and the stranger identification accuracy is above 91%. In addition, CareFi [70] and RDFID [77] can also realize stranger recognition.

4.1.2. Activity-Based. Activity-based user authentication has become increasingly popular due to its efficiency, scalability, and reliability. It can identify a user's identity when the user conducts some activities. As shown in Table 2, we list four typical activity-based applications. In this section, we investigate some of the latest activity-based identification instances.

As shown in Table 2, [53, 63, 67] can realize user authentication by daily activities. Reference [54] is an in-car driver authentication system based on CSI. Specifically, the stage of collecting CSI data lasts two months, from morning to night every day. The car was parked in 60 different locations,

Table 1: Gait-based user authentication applications.

System	Users	Signal/preprocessing	Experimental scene	Purpose/classification	Performance
WFID [62]	Corridor: 9 Laboratory: 6	Amplitude/PCA	Corridor, laboratory (155 m^2)	Identity recognition/SVM	6 people: 93.1% 9 people: 91.9%
WiFi-ID [65]	20	Amplitude/Butterworth filter, CWT	Corridor	Identity recognition/SAC	2 to 6 people: 93% to 77%
FreeSense [51]	9	Amplitude/PCA, DWT, low-pass filter	A smart home environment (6 m × 5 m)	Identity recognition/KNN, DTW	2 to 6 people: 94.5% to 88.9%
WiWho [58]	20	Amplitude/multipath removal, band-pass filter	Three indoor environments	Identity recognition/decision tree	2 to 6 people: 92% to 80%
WifiU [69]	50	Amplitude/PCA, STFT	A typical lab (50 m^2)	Identity recognition/LibSVM with RBF kernel	50 people: top 1: 79.28% Top 2: 89.52% Top 3: 93.05%
Jakkala et al. [71]	30	Amplitude/Hanning window	An office	Identity recognition/DCNN	30 people: 97.12 ± 1.13%
AutoID [72]	20	Amplitude/DWT	A conference room (5 m × 7 m), an office zone (5.6 m × 9 m), a bedroom apartment (7.5 m × 8 m)	Identity recognition/convex clustered concurrent Shapelet learning	20 people: 91%
Nipu et al. [73]	5	Amplitude/Butterworth low-pass filter	An opened room	Identity recognition/decision tree, random Forest	2 to 5 people: 95% to 84% (decision tree), 97.5% to 78% (random Forest)
Neural Wave [74]	24	Amplitude and phase/WT, IWT, and PCA	A typical indoor laboratory	Identity recognition/1-D ConvNet, called RadioNet (23 layers)	24 people: 87.76% ± 2.14%
Wide [75]	10	Amplitude/PCA	A laboratory	Identity recognition/SVM	Open scene: 98.7% No interference: 100% eliminate scene disturbances: 99.7%
Nkabiti et al. [76]	7	Amplitude and phase/Chebyshev filter	Dormitory room (6 m × 4 m) and hallway	Identity recognition/LSTM-RNN	Dormitory: 95.5% Hallway: 96.3%
Wii [59]	8	Amplitude and phase/PCA, CWT, low-pass filter	A meeting room (5 m × 4 m)	Identity recognition stranger identification/SVM, GMM	2 to 6 people: 98.7% to 90.9% Stranger identification accuracy: about 93% of 2 strangers
CareFi [70]	16	Amplitude/low-pass filter, PCA, STFT	A typical meeting room (9 m × 9 m), an apartment (8 m × 9 m)	Stranger identification/SVM	Intruder detection: more than 87.2%
RDFID [77]	4	Amplitude and phase/PCA, CWT	A meeting room (5 m × 4 m), a living room (5 m × 4 m), a large office (10 m × 6 m)	Stranger identification/SVM, GMM	Stranger identification accuracy: around 79% FN: around 2% FP: around 2%
HumanFi [64]	24	Amplitude and phase/Butterworth filter, a method proposed in [78]	The doorway of an office, the middle of an office	Identity recognition/LSTM	24 people: 96%
Deep-WiID [52]	15	Amplitude	Hall, lab	Identity recognition/GRU, average pooling	2 to 6 people: 99.7% to 97.7% 15 people: 92.5%
CSIID [79]	6	Amplitude	An indoor environment	Identity recognition/convolution layer, LSTM	2 to 6 people: 97.4% to 94.8%

Table 1: Continued.

System	Users	Signal/preprocessing	Experimental scene	Purpose/classification	Performance
WiDIGR [80]	60	Amplitude/band-pass filter, PCA	A laboratory, an empty room, and an apartment	Identity recognition/SVM	3 to 6 people: 92.83% to 78.28%
Gate-ID [81]	20	Amplitude/silence removal algorithm [65]	A room	Identity recognition/ResNet and bi-LSTM	6 to 20 people: 90.7% to 75.7%

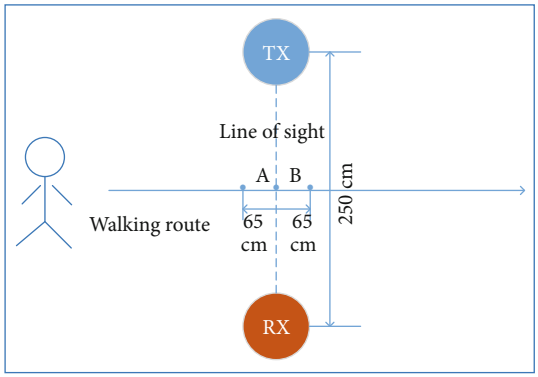

Figure 8: The regulation of walking [51].

and the data were collected in each position. Furthermore, the authors gathered CSI data in an empty car before collecting experimental data for three months. The locations of the signal transmitter, receiver, and driver are shown in Figure 9. Finally, this driver authentication system can achieve two functions. Two trained drivers can be distinguished, and the other can identify an illegal driver. The two situations achieved accuracies of 99.3% and 90.66%, respectively.

4.1.3. Gesture-Based. Gesture-based user authentication systems can identify different people according to the unique hand gestures of everyone. In other words, gesture-based identification approaches can recognize more fine-grained behavior. In Table 3, we list typical gesture-based user authentication applications.

For example, FingerPass [55] is a CSI-based identification system using finger gestures. It utilized CSI amplitude to recognize finger motion and employed phase information of CSI to authenticate identity. This system includes finger gesture data collection, signal preprocessing, finger gesture detection and recognition, and user authentication. The collected data were composed of eight usual finger gestures, as shown in Figure 10. In preprocessing, the authors adopted IFFT (inverse fast Fourier transform) and Butterworth filter. In addition, they realized finger gesture detection and recognition by signal segmentation and machine learning technology SVM. The authors mainly realized signal segmentation by utilizing amplitude differential. Specifically, they compared the amplitude differential with a predefined threshold using a sliding window to determine the starting and ending points of a gesture. In user authentication, a unique feature was extracted by LSTM-based DNN to identify legal users or illegal users. Afterward, this system applied a support vector domain description (SVDD) model to realize user verification. Eventually, FingerPass achieved an average accuracy of 91.4%. In addition, Wi-Sign [82] and WiID [83] are typical gesture-based user authentication systems. Wi-Sign can realize authentication by user sign with his/her finger in a designated location on the login device to prove the second factor (the first factor is username + password). WiID realized authentication by 7 gestures, i.e., push and pull arm (PP), circular arm motion (CA), waving arm motion (WA), kicking (KK), open and close door (OC), raising and lowering both arms (RL), and extending both arms forward, and then moving to sides (EM).

4.2. Stillness-Based Applications. Gait, activity, and gestures are typical human actions that can change CSI signal propagation and generate dynamic CSI profiles. All of them are action-based user authentication. These approaches require people to carry out some actions to determine identity. As a result, this approach may bring about inconvenience in some scenarios. Therefore, there is a pressing need for action-free user authentication. Currently, action-free user authentication research has achieved some progress, and some related applications have been developed. However, since it is difficult to detect subtle motions, there are a few stillness-based user authentication applications currently. Next, we introduce some action-free identification approaches, i.e., stillness-based user authentication. Specific stillness-based applications are listed in Table 4.

WiPIN [56] is an action-free system that can realize user authentication when people keep standing up. It collected the CSI signals and analyzed them by considering people's body components, including water rate, fat rate, muscle rate, and bone rate. The authors found that a user will generate unique CSI signals when standing in the WiFi area due to the permeability, permittivity, and propagation distance of people's body layers. They used the Butterworth filter to remove noise and applied IFFT to eliminate the multipath effect. In feature extraction, they selected 30 time-domain features and nine frequency-domain features. Finally, SVM was used to identify a specific identity. WiPIN can identify 100% of two people and 92% of 30 people. Different from WiPIN [56], Abyaneh et al. [57] also proposed a stillness-based user authentication system that can identify the user in a specific location. It achieved user authentication by the combination of location and user. In addition, some stillness-based systems applied respiration and lip motion, such as references [61, 68].

Different user authentication applications apply many suitable actions based on specific requirements. The common actions contain gait, activity, or gestures because they can be

Table 2: Activity-based user authentication applications.

System	Users	Signal/preprocessing	Experimental scene	Purpose/classification	Performance
WiAU [53]	Office: 12 Corridor: 14 (two users are twins)	Amplitude/Butterworth low-pass filter	An office and three corridors of different floors	Identity recognition stranger identification/CNN, ResNet	Legal user (12 or 14 people): 98% Illegal user: 92%
WiID [67]	10	Amplitude and phase/low-pass filter, PCA, and DWT	Two laboratories	Identity recognition/SVM and HMM	10 people: 90%
Shi et al. [63]	Office: 11 Apartment: 5	Amplitude and phase/band-pass filter	An office (26 ft × 14 ft) An apartment (36 ft × 22 ft)	Identity recognition stranger identification/DNN, SVM	Walking activities: 94% Stationary activities: 91% Illegal user: 89.7%
Regani et al. [54]	5	Phase/PCA	In-car scenarios	Identity recognition stranger identification/KNN, linear SVM, SVM-RBF, and NN	Single driver: 90.66% Two drivers: 99.36%

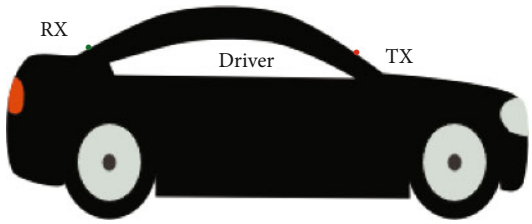

Figure 9: Experimental environment [54].

conducted easily and can generate unique CSI variation for each user. In contrast, some applications are action-free and usually can be described as biometric features. Therefore, they cannot be widely employed compared with large range motion. However, these systems have special advantages since they do not require conducting any actions. Compared to stillness-based authentication, action-based user authentication can realize better performance. In particular, gait-based user authentication is the most commonly used in all user authentication systems and has a better result in identifying the number of people and accuracy because it can be used in many scenes in daily life and has high application value. Overall, most existing user authentication applications have achieved considerable performance, but there are still many factors that can influence identification accuracy.

5. Discussion

In this section, we discuss some essential factors that establish crucial characteristics of the system and present some insights into the development of user authentication using CSI signals. We hope this discussion can provide some helpful information for developers. We also analyze the major causes affecting system performance.

From the signal processing aspect, most systems employ an Intel 5300 NIC to collect CSI data. The signal of CSI involves amplitude and phase. Most applications employ amplitude features because they can depict changes in signal power and can be utilized to establish the relationship between the signal profile and human identity. In addition, some systems apply phase features because they are sensitive to fine-grained actions and have excellent real-time properties. However, it also has some weaknesses in terms of the periodicity of the signal and sensitivity to noise. The CSI phase can be affected by SFO (sampling frequency offset) and CFO (carrier frequency offset), which decreases the accuracy of measurement data. Based on the analysis, the system usually applies some preprocessing methods to eliminate the noise from the test environment and other people nearby. The main methods include PCA, Butterworth low-pass filter, CWT, DWT, and IFFT.

From the perspective of actions conducted, most applications employ gait because it can generate evident changes in CSI, which facilitates data measurement and feature extraction. In addition, human gait usually has stable unique features, which have been confirmed and can be utilized to check human identity. The hand gesture is another action employed in these systems since the signal variation from the waving hand is also unique for each person and can be identified. In addition, other actions, such as respiration and lip motion, are also employed by a few systems.

From the authentication method aspect, SVM is the most widespread recognition approach employed in authentication systems due to its excellent classification performance for complex data. In addition, KNN and DTW are also employed in some applications. The utilization of CNN and RNN is emerging in a few systems. In the classification technique, the majority of recognition methods are pattern-based algorithms, and the minority of them are deep learning-based. We deem that the proportion of deep learning will increase with wide application of user authentication.

From a system performance aspect, most tests are conducted in 2-4 rooms to evaluate system performance. The number of participants varies significantly from 4 to 50. Most

Table 3: Gesture-based user authentication applications.

System	Users	Signal/preprocessing	Experimental scene	Purpose/classification	Performance
Wi-Sign [82]	14	Amplitude/PCA Butterworth low-pass filter	A typical office room (5 m × 3.5 m)	Identity recognition, stranger identification/SVM	14 people TPR: 79% Intruder detection TNR: 86%
WiID [83]	21	Amplitude/PCA	A lab (400 ft^2), an office (150 ft^2), a living room (192 ft^2), and a bedroom (154 ft^2)	Identity recognition/SVDE	An average cross-validation accuracy of 5 users: 92.8% in four environments
Finger Pass [55]	7	Amplitude and phase/IFFT	A living room (5.8 m × 4.2 m), a bedroom (3.8 m × 3.4 m), and a kitchen (3.4 m × 2.2 m)	Identity recognition, stranger identification/SVM, LSTM-based DNN	7 people: 91.4%

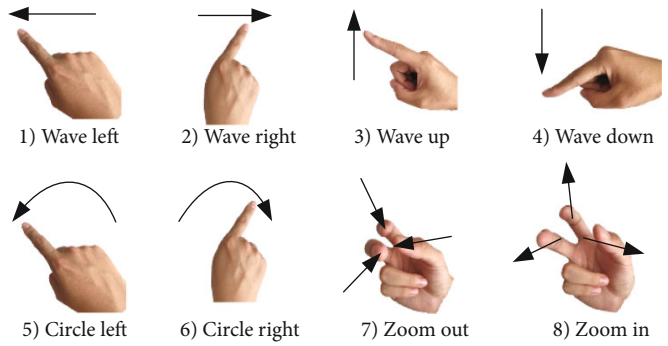

Figure 10: The eight different finger gestures [55].

of them can recognize fewer than 20 users, while a few systems can identify 30 or 50 users. Based on our conclusion, the system achieves noteworthy identification results if it can recognize up to ten users based on CSI. Some systems can identify close to 20 users, which is an excellent result. A few systems can determine user authentication from 30 or 50 participants, which is an extraordinary accomplishment using CSI. These achievements have a competitive edge compared with other systems using various signals since the CSI signal can provide long-term and nonintrusive recognition patterns without privacy violation. From the recognition accuracy view, we find that most systems achieve more than 90% recognition accuracy, and some systems accomplish near 90% identification accuracy for more than 20 participants. The results indicate that the principle of user authentication based on CSI is reliable. We can apply these systems in empirical scenarios if the number of participants meets our requirements.

In summary, the state-of-the-art studies in this survey explore the CSI dynamics caused by different users and leverage them to realize user authentication. Extracting specific features that represent the user identity and separating him/her from a group are challenging problems. We discuss the key components affecting system performance and evaluate the system from the implementation view. We deem that many factors should be considered when developing a user authentication system. The essential elements of a system include the number of participants, types of user actions, and recognition technique, which largely determine the system performance. With the introduction of a novel CSI dynamic model and recognition methods, the recognition accuracy will increasingly improve, and the user size will gradually increase, which will greatly enrich the research approach and expand the application field.

6. Issues and Future Research Trends

In this section, we present some issues and research trends based on user authentication applications. They involve some essential research topics and crucial techniques. We present them from the following aspects, including through-the-wall scenario, robustness, and more application scenarios.

6.1. Through-the-Wall User Authentication. Through-the-wall (TTW) user authentication using CSI is an important research topic and has wide application scenarios, such as emergency rescue and health monitoring for the elderly [87]. Similarly, TTW user authentication also recognizes personal identity using the characteristics of CSI. Specifically, they leverage the penetration capability of the CSI signal to implement TTW individual authentication. However, eliminating the effect of the wall on the CSI signal is a challenging problem. For example, Xu et al. [88] proposed a user authentication system through the wall using the time-reversal (TR) technique to obtain radio biometrics. Radio biometrics are defined as the wireless signal attention and variation containing identity features when a person is located within the signal coverage. Raw CSI is a high-dimensional signal, and the CSI profile distorts after traveling the wall. The TR technique is applied to capture CSI signals reflecting human radio

Table 4: Stillness-based user authentication applications.

System	Users	Signal/preprocessing	Experimental scene	Purpose/classification	Performance
Liu et al. [84]	12 locations	Amplitude/temporal correlation analysis	A laboratory (11 m × 12 m) and an apartment (11 m × 6 m)	Identity recognition stranger identification/SVM	Attack detection: 92% Authentication accuracy: 98.4%
WiPIN [56]	30	Amplitude/Butterworth filter	A room (5 m × 6 m)	Identity recognition/SVM	Two people: 100% 30 people: 92%
Abyaneh et al. [57]	11 locations	Amplitude and phase	An apartment, a garage, and the ramp	Identity recognition/LocNet	Apartment: 85.35% Garage: 98.5%
BodyPIN [85]	30	Amplitude and phase/Butterworth low-pass filter	A room (5 m × 6 m)	Identity recognition/SVM	30 users: 92%
Liu et al. [61]	20	Amplitude/EMD-based filter	A university office (17 ft × 19 ft)	Identity recognition, stranger identification/KNN	20 people: 93% Random attacks: 92.14% with 5% FP Imitation attacks: 89.24% with 5% FP
Wang et al. [86]	10	Amplitude/PCA	A laboratory (9 m × 12 m)	Identity recognition/softmax regression	10 people: 97.5% (respiration) 90.4% (gait)
CP-ID [66]	6	Phase/PCA	A typical office (5 m × 3.5 m)	Identity recognition/SVM	From 2 to 5 people: 84% to 65%
BioID [68]	5	Amplitude/Butterworth low-pass filter, PCA, and DWT	An office	Identity recognition/KNN	5 people: 90%

biometric information and identify different individuals. In addition, the authors employ many approaches to extract representative CSI features, including phase alignment and background subtraction algorithms. Overall, the key to TTW user authentication is how to remove the fluctuation of the CSI signal from the effect of the wall. In addition, many factors also affect the recognition results, including different obstructions, person positions, device deployment, and the number of users. Therefore, the general effect of walls on recognition accuracy is still not clear, and more application environments should be tested to validate the availability of the TTW user authentication system. We deem that TTW user authentication has a wide range of fields when the impact of the wall can be eliminated effectively.

6.2. Robustness of User Authentication System. The robustness of user authentication describes the system's performance under various test conditions. It includes two aspects. The first evaluates the authentication accuracy for different environments, such as offices, libraries, rooms, homes, apartments, and corridors. The second tests recognition performance for different user motions. We discuss the effect of two conditions on system performance. First, for different environments, many applications validate system performance in different test environments. For instance, experiments are usually performed in 2-4 rooms [58, 63]. The algorithms usually work well in test environments. However, we expect the algorithms to work in different scenarios and accommodate the changes in new environments. Second, most user authentication systems are aimed at specific motions, such as gaits, gestures, or other actions. Some applications propose a general algorithm that is suitable for many different gestures, such as gestures, movements, or a mixture of continuous behaviors [53]. The general approaches usually leverage deep neural networks to implement their availability for different actions. The key reason can be interpreted as follows. Most applications need to conduct specific actions and analyze the corresponding data. Therefore, these approaches are related to specific actions. In contrast, deep learning approaches have a strong capability of general feature extraction, and various types of data can be used due to their powerful processing capacity. The robustness of various motions usually comes from applications using deep learning approaches. Overall, we have to consider the problem that no robust systems are suitable for all different environments or different motions. This problem may be mitigated by extracting more accurate identity features.

6.3. More Potential Application Scenarios. Currently, most applications determine user identity in specific spaces, such as corridors, labs, apartments, offices, and meeting rooms. We deem that these systems can be expanded in many application fields. For instance, there is an interesting application to check driver identity [54], which has many evident differences compared with the general test environments. In addition, different applications may require different actions and feature extraction. For example, reference [89] leverages

respiratory features extracted from CSI to implement user authentication. It utilizes waveform transformation to analyze respiration signals and deep neural networks to identify a user. Another amazing user authentication example using CSI is XModal-ID [90]. Based on the user gaits, it fulfills a challenging and promising task that the system can judge whether a person is a target given the WiFi signal measured and the corresponding user walking in an unknown field and a video segmentation of a walking user in another field area. It establishes the relationship of video gait with CSI signal variation and determines whether the user is the subject based on the CSI fluctuation from another video area. In addition, many systems combine user authentication with other functions to achieve more useful applications, such as user authentication and gesture recognition [91] and user authentication, activity classification, and tracking [92]. These different scenarios can apply user authentication to implement nonintrusive user authentication.

7. Conclusions

The WiFi CSI signal contains plenty of channel information of wireless communication links for evaluating wireless link states and improving communication quality. Obstructing the communication path will lead to evident signal fluctuation. In particular, the communication path will generate a distinct profile of CSI variation due to the influence of users and surrounding environments. The crucial characteristic can be leveraged for user authentication. Based on this principle, a useful theory has been proposed, and typical user authentication applications have been implemented. User authentication technology based on the WiFi CSI signal brings great convenience due to its nonintrusive characteristics and wide availability of the WiFi signal. We investigate state-of-the-art systems and analyze their characteristics from many aspects. The signal processing procedures of user authentication include signal selection and preprocessing, feature extraction, and classification. Typical classification approaches involve machine learning and deep learning methods. We find that deep learning approaches are becoming popular due to powerful hidden feature extraction and accurate recognition. Based on the user motion state, we classify these existing user authentication applications into two categories: action-based and stillness-based applications. We elaborate on the core characteristics of these applications. We find that action-based user authentication has been widely employed since CSI variation caused by coarse-grained actions can be easily measured and identified. In addition, stillness-based user authentication has rarely been applied because CSI variation caused by fine-grained actions is difficult to measure. However, it also has many potential applications since it does not require users to perform any actions. By analyzing the existing user authentication system, we summarized the factors affecting user authentication performance and pointed out future development directions. We deem that user authentication will realize better performance if we can address some problems, such as through-the-wall conditions, robustness, and more potential application scenarios.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the Shandong University Youth Innovation Supporting Program (2019KJN020), in part by the Tai'shan Scholar Engineering Construction Fund of Shandong Province of China, in part by the Qingdao Postdoctoral Applied Research Project under Grant 2015180, and the Key Research and Development Plan of Shandong Province (Public Welfare Special) Project under 2018GHY115022.

References

[1] M. Alafeef and M. Fraiwan, "Smartphone-based respiratory rate estimation using photoplethysmographic imaging and discrete wavelet transform," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 2, pp. 693–703, 2020.

[2] B. Fang, N. D. Lane, M. Zhang, A. Boran, and F. Kawsar, "BodyScan: enabling radio-based sensing on wearable devices for contactless activity and vital sign monitoring," in *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services*, pp. 97–110, Singapore, Singapore, 2016.

[3] A. Jalal, S. Kamal, and D. Kim, "A depth video sensor-based life-logging human activity recognition system for elderly care in smart indoor environments," *Sensors*, vol. 14, no. 7, pp. 11735–11759, 2014.

[4] S. Herath, M. Harandi, and F. Porikli, "Going deeper into action recognition: a survey," *Image & Vision Computing*, vol. 60, pp. 4–21, 2017.

[5] A. Núñez-Marcos, G. Azkune, and I. Arganda-Carreras, "Vision-based fall detection with convolutional neural networks," *Wireless Communications and Mobile Computing*, vol. 2017, Article ID 9474806, 16 pages, 2017.

[6] C. Zhang, Q. Xue, A. Waghmare et al., "SoundTrak: continuous 3D tracking of a finger using active acoustics," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 1, no. 2, Article ID 30, 25 pages, 2017.

[7] Z. Wang, Y. Hou, K. Jiang et al., "A survey on human behavior recognition using smartphone-based ultrasonic signal," *IEEE Access*, vol. 7, pp. 100581–100604, 2019.

[8] Z. Wang, Y. Hou, K. Jiang et al., "Hand gesture recognition based on active ultrasonic sensing of smartphone: a survey," *IEEE Access*, vol. 7, pp. 111897–111922, 2019.

[9] W. Ruan, Q. Z. Sheng, and L. Yang, "AudioGest: enabling fine-grained hand gesture detection by decoding echo signal," in *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pp. 474–485, Heidelberg, Germany, 2016.

[10] T. Li, C. An, T. Zhao, A. T. Campbell, and Z. Xia, "Human sensing using visible light communication," in *Proceedings of*

the 21st Annual International Conference on Mobile Computing & Networking, pp. 331–344, Paris, France, 2015.

[11] T. Li, L. Qiang, and Z. Xia, "Practical human sensing in the light," in *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services*, pp. 71–84, Singapore, Singapore, 2016.

[12] Y. Zou, J. Xiao, J. Han, K. Wu, Y. Li, and L. M. Ni, "GRfid: a device-free RFID-based gesture recognition system," *IEEE Transactions on Mobile Computing*, vol. 16, no. 2, pp. 381–393, 2017.

[13] C. Wang, J. Liu, and Y. Chen, "Multi-touch in the air: device-free finger tracking and gesture recognition via COTS RFID," in *IEEE INFOCOM 2018- IEEE Conference on Computer Communications*, pp. 1691–1699, Honolulu, HI, USA, 2018.

[14] L. Yao, Q. Z. Sheng, X. Li et al., "Compressive representation for device-free activity recognition with passive RFID signal strength," *IEEE Transactions on Mobile Computing*, vol. 17, no. 2, pp. 293–306, 2017.

[15] I. Milani, F. Colone, C. Bongioanni, and P. Lombardo, "WiFi emission-based vs passive radar localization of human targets," in *2018 IEEE radar Conference (RadarConf18)*, pp. 1311–1316, Oklahoma City, OK, USA, 2018.

[16] J. Wang, Q. Gao, Y. Yu, P. Cheng, L. Wu, and H. Wang, "Robust device-free wireless localization based on differential RSS measurements," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 12, pp. 5943–5952, 2013.

[17] Y. Guo, K. Huang, N. Jiang, X. Guo, Y. Li, and G. Wang, "An exponential-Rayleigh model for RSS-based device-free localization and tracking," *IEEE Transactions on Mobile Computing*, vol. 14, no. 3, pp. 484–494, 2015.

[18] K. Wu, J. Xiao, Y. Yi, D. Chen, X. Luo, and L. M. Ni, "CSI-based indoor localization," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 7, pp. 1300–1309, 2013.

[19] Z.-P. Jiang, W. Xi, X. Li et al., "Communicating is crowdsourcing: Wi-fi indoor localization with CSI-based speed estimation," *Journal of Computer Science and Technology*, vol. 29, no. 4, pp. 589–604, 2014.

[20] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, "Predictable 802.11 packet delivery from wireless channel measurements," *SIGCOMM Comput. Commun. Rev.*, vol. 40, no. 4, pp. 159–170, 2010.

[21] Y. Xie, Z. Li, and M. Li, "Precise power delay profiling with commodity WiFi," in *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*, pp. 1342–1355, Paris, France, 2015.

[22] F. Gringoli, M. Schulz, J. Link, and M. Hollick, "Free your CSI: a channel state information extraction platform for modern Wi-Fi chipsets," in *the 13th International Workshop*, pp. 21–28, Los Cabos, Mexico, 2019.

[23] M. Atif, S. Muralidharan, H. Ko, and B. Yoo, "Wi-ESP—a tool for CSI-based device-free Wi-Fi sensing (DFWS)," *Journal of Computational Design and Engineering*, vol. 7, no. 5, pp. 644–656, 2020.

[24] Z. Wang, K. Jiang, Y. Hou et al., "A survey on human behavior recognition using channel state information," *IEEE Access*, vol. 7, pp. 155986–156024, 2019.

[25] J. Liu, H. Liu, Y. Chen, Y. Wang, and C. Wang, "Wireless sensing for human activity: a survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1629–1645, 2019.

[26] J. Liu, G. Teng, and F. Hong, "Human activity sensing with wireless signals: a survey," *Sensors*, vol. 20, no. 4, Article ID 1210, 45 pages, 2020.

[27] P. Gallo and S. Mangione, "RSS-eye: human-assisted indoor localization without radio maps," in *2015 IEEE International Conference on Communications (ICC)*, pp. 1553–1558, London, UK, 2015.

[28] B. Mager, P. Lundrigan, and N. Patwari, "Fingerprint-based device-free localization performance in changing environments," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 11, pp. 2429–2438, 2015.

[29] P. Xiang, P. Ji, and D. Zhang, "Enhance RSS-based indoor localization accuracy by leveraging environmental physical features," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 8956757, 8 pages, 2018.

[30] K. Dong, Z. Ling, X. Xia, H. Ye, W. Wu, and M. Yang, "Dealing with insufficient location fingerprints in Wi-Fi based indoor location fingerprinting," *Wireless Communications and Mobile Computing*, vol. 2017, Article ID 1268515, 11 pages, 2017.

[31] S. Imran and Y.-B. Ko, "A novel indoor positioning system using kernel local discriminant analysis in Internet-of-Things," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 2976751, 9 pages, 2018.

[32] J. Bai, Y. Sun, W. Meng, and C. Li, "Wi-Fi fingerprint-based indoor mobile user localization using deep learning," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 6660990, 12 pages, 2021.

[33] C. Xiao, D. Han, Y. Ma, and Z. Qin, "CsiGAN: robust channel state information-based activity recognition with GANs," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10191–10204, 2019.

[34] Z. Chen, L. Zhang, C. Jiang, Z. Cao, and W. Cui, "WiFi CSI based passive human activity recognition using attention based BLSTM," *IEEE Transactions on Mobile Computing*, vol. 18, no. 11, pp. 2714–2724, 2018.

[35] Q. Zhou, C. Wu, J. Xing, S. Zhao, and Q. Yang, "Enabling non-invasive physical assault monitoring in smart school with commercial Wi-Fi devices," *Wireless Communications and Mobile Computing*, vol. 2019, Article ID 8186573, 14 pages, 2019.

[36] D. L. Hall, R. M. Narayanan, E. H. Lenzing, and D. M. Jenkins, "Passive vector sensing for non-cooperative emitter localization in indoor environments," *Electronics*, vol. 7, no. 12, pp. 442–466, 2018.

[37] C. Han, W. Xun, L. Sun, Z. Lin, and J. Guo, "DSCP: depth-wise separable convolution-based passive indoor localization using CSI fingerprint," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 8821129, 17 pages, 2021.

[38] X. Yang, F. Xiong, Y. Shao, and Q. Niu, "WmFall: WiFi-based multistage fall detection with channel state information," *International Journal of Distributed Sensor Networks*, vol. 14, 10 pages, 2018.

[39] S. Palipana, D. Rojas, P. Agrawal, and D. Pesch, "FallDeFi: ubiquitous fall detection using commodity Wi-Fi devices," *PACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 1, no. 4, Article ID 155, 25 pages, 2017.

[40] K. Ali, A. X. Liu, W. Wang, and M. Shahzad, "Keystroke recognition using WiFi signals," in *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*, pp. 90–102, Paris, France, 2015.

[41] F. Li, X. Wang, H. Chen, K. Sharif, and Y. Wang, "ClickLeak: keystroke leaks through multimodal sensors in cyber-physical social networks," *IEEE Access*, vol. 5, pp. 27311–27321, 2017.

[42] C. Chen, Y. Han, Y. Chen et al., "TR-BREATH: time-reversal breathing rate estimation and detection," *IEEE Transactions on Biomedical Engineering*, vol. 65, no. 3, pp. 489–501, 2018.

[43] Y. Zeng, D. Wu, J. Xiong, E. Yi, R. Gao, and D. Zhang, "FarSense: pushing the range limit of WiFi-based respiration sensing with CSI ratio of two antennas," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 3, no. 3, Article ID 121, 27 pages, 2019.

[44] X. Zheng, J. Wang, L. Shangguan, Z. Zhou, and Y. Liu, "Smokey: ubiquitous smoking detection with commercial WiFi infrastructures," in *IEEE INFOCOM 2016- The 35th Annual IEEE International Conference on Computer Communications*, pp. 1–9, San Francisco, CA, USA, 2016.

[45] W. Xi, J. Zhao, and X. Y. Li, "Electronic frog eye: counting crowd using WiFi," in *IEEE INFOCOM 2014- IEEE Conference on Computer Communications*, pp. 361–369, Toronto, ON, Canada, 2014.

[46] S. Doong, "Counting human flow with deep neural network," in *Proceedings of the 51st Hawaii International Conference on System Sciences*, pp. 799–808, Big Island, Hawaii, 2018.

[47] Z. Tian, J. Wang, X. Yang, and M. Zhou, "WiCatch: a Wi-fi based hand gesture recognition system," *IEEE Access*, vol. 6, pp. 16911–16923, 2018.

[48] H. F. Thariq Ahmed, H. Ahmad, and A. CV, "Device free human gesture recognition using Wi-Fi CSI: a survey," *Engineering Applications of Artificial Intelligence*, vol. 87, Article ID 103281, 19 pages, 2020.

[49] X. Dang, Y. Liu, Z. Hao, X. Tang, and C. Shao, "Air gesture recognition using WLAN physical layer information," *Wireless Communications and Mobile Computing*, vol. 2020, Article ID 8546237, 14 pages, 2020.

[50] S. W. Shah and S. S. Kanhere, "Recent trends in user authentication – a survey," *IEEE Access*, vol. 7, pp. 112505–112519, 2019.

[51] T. Xin, B. Guo, and Z. Wang, "FreeSense: indoor human identification with Wi-Fi signals," *IEEE global Communications Conference (GLOBECOM)*, 2016, pp. 1–7, Washington, DC, USA, 2016.

[52] Z. Zhou, C. Liu, and X. Yu, "Deep-WiID: WiFi-based contactless human identification via deep learning," in *2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation*, pp. 877–884, Leicester, United Kingdom, United Kingdom, 2019.

[53] C. Lin, J. Hu, and Y. Sun, "WiAU: an accurate device-free authentication system with ResNet," in *2018 15th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, pp. 1–9, Hong Kong, China, 2018.

[54] S. D. Regani, Q. Xu, B. Wang, M. Wu, and K. J. R. Liu, "In-car driver authentication using wireless sensing," in *ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 7595–7599, Brighton, United Kingdom, United Kingdom, 2019.

[55] H. Kong, L. Lu, J. Yu et al., "FingerPass: finger gesture-based continuous user authentication for smart homes using commodity WiFi," in *Proceedings of the Twentieth ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pp. 201–210, Catania, Italy, 2019.

[56] F. Wang, J. Han, Z. Dai, H. Ding, and D. Huang, "WiPIN: operation-free passive person identification using WiFi signals," in *2019 IEEE global Communications Conference*, pp. 1–11, Waikoloa, HI, USA, 2019.

[57] A. Yazdani Abyaneh, A. Hosein Gharari Foumani, and V. Pourahmadi, "CSI-based authentication: extracting stable features using deep neural networks," *Transaction on Emerging Telecommunications Technologies*, vol. 31, no. 2, Article ID e3795, 12 pages, 2019.

[58] Y. Zeng, P. H. Pathak, and P. Mohapatra, "WiWho: WiFi-based person identification in smart spaces," in *2016 15th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, pp. 1–12, Vienna, Austria, 2016.

[59] J. Lv, W. Yang, and D. Man, "Device-free passive identity identification via WiFi signals," *Sensors*, vol. 17, no. 11, pp. 2520–2536, 2017.

[60] X. Yang, "IEEE 802.11n: enhancements for higher throughput in wireless LANs," *IEEE Wireless Communications*, vol. 12, no. 6, pp. 82–91, 2005.

[61] J. Liu, Y. Dong, Y. Chen, Y. Wang, and T. Zhao, "Leveraging breathing for continuous user authentication," in *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*, pp. 786–788, New Delhi, India, 2018.

[62] F. Hong, X. Wang, and Y. Yang, "WFID: passive device-free human identification using WiFi signal," in *Proceedings of the 13th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, pp. 47–56, Hiroshima, Japan, 2016.

[63] C. Shi, J. Liu, H. Liu, and Y. Chen, "Smart user authentication through actuation of daily activities leveraging WiFi-enabled IoT," in *Proceedings of the 18th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pp. 1–10, Chennai, India, 2017.

[64] X. Ming, H. Feng, and Q. Bu, "HumanFi: WiFi-based human identification using recurrent neural network," in *2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation*, pp. 640–647, Leicester, United Kingdom, United Kingdom, 2019.

[65] J. Zhang, B. Wei, W. Hu, and S. S. Kanhere, "WiFi-ID: human identification using WiFi signal," in *2016 International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pp. 75–82, Washington, DC, USA, 2016.

[66] S. W. Shah and S. S. Kanhere, "Smart user identification using cardiopulmonary activity," *Pervasive and Mobile Computing*, vol. 58, Article ID 101024, 20 pages, 2019.

[67] R. Zheng, Y. Zhao, and B. Chen, "Device-free and robust user identification in smart environment using WiFi signal," in *2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications (ISPA/IUCC)*, pp. 1039–1046, Guangzhou, China, 2017.

[68] Z. Zhao, Z. Zhao, and G. Min, "Non-intrusive biometric identification for personalized computing using wireless big data," in *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation*

(SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), pp. 901–908, Guangzhou, China, 2018.

[69] W. Wang, A. X. Liu, and M. Shahzad, "Gait recognition using wifi signals," in *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pp. 363–373, Heidelberg, Germany, 2016.

[70] D. Zhu, N. Pang, W. Feng, M. Al-Khiza'ay, and Y. Ma, "Device-free intruder sensing leveraging fine-grained physical layer signatures.," in *In Knowledge Science, Engineering and Management, Springer International Publishing: Cham*, vol. 10412, pp. 183–194, Germany, 2017.

[71] K. Jakkala, B. Arupjyoti, Z. Sun, P. Wang, and Z. Cheng, "Deep CSI learning for gait biometric sensing and recognition," 2019, https://arxiv.org/abs/1902.02300.

[72] H. Zou, Y. Zhou, and J. Yang, "WiFi-based human identification via convex tensor shapelet learning," in *The Thirty-Second AAAI Conference on Artificial Intelligence*, pp. 1711–1718, New Orleans, Louisiana, USA, 2018.

[73] M. N. A. Nipu and S. Talukder, *Human Identification Using Wifi Signal*, BRAC University, Bangladesh, 2017.

[74] A. Pokkunuru, K. Jakkala, A. Bhuyan, P. Wang, and Z. Sun, "NeuralWave: gait-based user identification through commodity WiFi and deep learning," in *IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society*, pp. 758–765, Washington, DC, USA, 2018.

[75] C. Lin and M. S. Obaidat, "Behavioral biometrics based on human-computer interaction devices," in *In Biometric-Based Physical and Cybersecurity Systems*, pp. 189–209, Springer International Publishing: Cham, Germany, 2018.

[76] K. P. Nkabiti, Y. Chen, K. Sultan, and B. Armand, "A deep bidirectional LSTM recurrent neural networks for identifying humans indoors using channel state information," in *2019 28th wireless and optical Communications Conference (WOCC)*, pp. 1–5, Beijing, China, 2019.

[77] J. Lv, D. Man, W. Yang, L. Gong, X. du, and M. Yu, "Robust device-free intrusion detection using physical layer information of WiFi signals," *Applied Sciences*, vol. 9, no. 1, pp. 175–191, 2019.

[78] M. Kotaru, K. Joshi, D. Bharadia, and S. Katti, "SpotFi," *SIGCOMM Comput. Commun. Rev.*, vol. 45, no. 4, pp. 269–282, 2015.

[79] D. Wang, Z. Zhou, X. Yu, and Y. Cao, "CSIID: WiFi-based human identification via deep learning," in *2019 14th International Conference on Computer Science & Education (ICCSE)*, pp. 326–330, Toronto, ON, Canada, 2019.

[80] L. Zhang, C. Wang, M. Ma, and D. Zhang, "WiDIGR: direction-independent gait recognition system using commercial Wi-Fi devices," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 1178–1191, 2020.

[81] J. Zhang, B. Wei, F. Wu et al., "Gate-ID: WiFi-based human identification irrespective of walking directions in smart home," *IEEE Internet of Things Journal*, vol. 8, no. 9, pp. 7610–7624, 2021.

[82] S. W. Shah and S. S. Kanhere, "Wi-Sign: device-free second factor user authentication," in *Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, pp. 135–144, New York, NY, USA, 2018.

[83] M. Shahzad and S. Zhang, "Augmenting user identification with WiFi based gesture recognition," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 2, no. 3, Article ID 134, 27 pages, 2018.

[84] H. Liu, Y. Wang, J. Liu, J. Yang, Y. Chen, and H. V. Poor, "Authenticating users through fine-grained channel information," *IEEE Transactions on Mobile Computing*, vol. 17, no. 2, pp. 251–264, 2018.

[85] F. Wang, Z. Li, and J. Han, "Continuous user authentication by contactless wireless sensing," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8323–8331, 2019.

[86] J. Wang, Y. Zhao, X. Fan, Q. Gao, X. Ma, and H. Wang, "Device-free identification using intrinsic CSI features," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 9, pp. 8571–8581, 2018.

[87] Z. Wang, K. Jiang, Y. Hou et al., "A survey on CSI-based human behavior recognition in through-the-wall scenario," *IEEE Access*, vol. 7, pp. 78772–78793, 2019.

[88] Q. Xu, Y. Chen, B. Wang, and K. J. R. Liu, "Radio biometrics: human recognition through a wall," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 5, pp. 1141–1155, 2017.

[89] J. Liu, Y. Chen, Y. Dong, Y. Wang, T. Zhao, and Y. D. Yao, "Continuous user verification via respiratory biometrics," in *IEEE INFOCOM 2020- IEEE Conference on Computer Communications*, pp. 1–10, Toronto, ON, Canada, 2020.

[90] B. Korany, C. Karanam, H. Cai, and Y. Mostofi, "XModal-ID: using WiFi for through-wall person identification from candidate video footage," in *The 25th Annual International Conference on Mobile Computing and Networking*, pp. 1–15, Mexico, 2019.

[91] C. Li, M. Liu, and Z. Cao, "WiHF: enable user identified gesture recognition with WiFi," in *IEEE INFOCOM 2020- IEEE Conference on Computer Communications*, pp. 586–595, Toronto, ON, Canada, 2020.

[92] V. Jayasundara, H. Jayasekara, T. Samarasinghe, and K. T. Hemachandra, "Device-free user authentication, activity classification and tracking using passive Wi-Fi sensing: a deep learning-based approach," *IEEE Sensors Journal*, vol. 20, no. 16, pp. 9329–9338, 2020.